Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.1 Теория информации»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2024

Рабочая программа дисциплины «*Б1.Д.В.1 Теория информации*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 8 от "25" марта 2024 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем — И.В. Влацкая
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
ст. преподаватель кафедры КБМОИС — Н.А. Заельская
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность — И.В. Влацкая
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
Н.Н. Бигалиева
личная подпись *расшифровка подписи*

Уполномоченный по качеству института
И.В. Крючкова
личная подпись *расшифровка подписи*

№ регистрации _____

© Заельская Н.А., 2024
© ОГУ, 2024

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:
изучение методов решения задач, связанных с процессами хранения и передачи информации в управляющих системах. Применение алгоритмов постановки задачи неравномерного побуквенного кодирования, постановки задачи универсального кодирования и наиболее эффективные способы универсального кодирования источников – методы Зива-Лемпела, а также их использования при решении практических задач.

Задачи:

- приобретение обучающимися знаний в области кодирования информации;
- получение представления о кодировании дискретных источников;
- получение студентами практических навыков при работе с алгоритмами кодирования источников.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательным дисциплинам (модулям) вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.10 Информатика, Б1.Д.Б.44.4 Теория передачи сигналов и сообщений*

Постреквизиты дисциплины: *Отсутствуют*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1-В-4 Применяет методы сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий для решения поставленных задач	**Знать:** Технологию кодирования дискретных источников. **Уметь:** Вычислять теоретико-информационные характеристики источников сообщений. **Владеть:** Навыками применения математического аппарата для решения прикладных теоретико-информационных задач.
ПК*-2 Формирование требований в защите информации в автоматизированных системах	ПК*-2-В-1 Умеет определять угрозы безопасности информации, обрабатываемой автоматизированной системой	**Знать:** Основные тенденции современного развития кодирования дискретных источников. **Уметь:** Решать задачи кодирования и декодирования. **Владеть:** Способностью к обобщению, анализу алгоритмов кодирования информации, постановке цели и задачи кодирования.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 академических часа).

Вид работы	Трудоемкость, академических часов	
	9 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**69,25**	**69,25**
Лекции (Л)	34	34
Лабораторные работы (ЛР)	34	34
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий);* *- изучение разделов курса «Теория информации» в системе электронного обучения;* *- подготовка к итоговому тестированию в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к коллоквиумам;* *- подготовка к рубежному контролю*.	**74,75**	**74,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 9 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Дискретные источники сообщений. Равномерное кодирование дискретного источника.	22	6	-	-	16
2	Неравномерное кодирование дискретных источников.	18	6	-	-	12
3	Побуквенное кодирование.	34	6	-	10	18
4	Неравномерное кодирование для стационарного источника.	28	8	-	6	14
5	Алгоритмы кодирования источников, применяемые в архиваторах.	42	8	-	18	16
	Итого:	144	34	-	34	76
	Всего:	144	34	-	34	76

4.2 Содержание разделов дисциплины

1 Дискретные источники сообщений. Равномерное кодирование дискретного источника.

Наука теория информации. Задачи теории информации. Структурная схема типичной системы передачи и хранения информации. Разделы теории информации.

Несовместные события. Совместно независимые события. Формула полной вероятности. Произведение множеств. Произведение вероятностных ансамблей. Условное распределение вероятностей на элементах множества. Математическое ожидание случайной величины.

Мера измерения информации. Случайные события. Требования к информационной мере. Собственная информация. Свойства собственной информации. Энтропия. Свойства энтропии. Последовательности зависимых сообщений. Условная собственная информация. Условная энтропия. Свойства условной энтропии.

Случайные процессы. Задание случайного процесса. Предположение о стационарности. Стационарный процесс. Числовые характеристики стационарных процессов. Дискретный постоянный источник. Цепь Маркова связанности s. Однородная марковская цепь. Простая цепь Маркова. Матрица переходных вероятностей. Стационарное распределение для цепи Маркова. Финальное распределение вероятностей. Необходимое и достаточное условие эргодичности. Одномерная энтропия источника. n-мерная энтропия источника. Энтропия на букву последовательности длинны n. Теорема устанавливающая некоторые свойства двух информационных мер $H_n(X)$ и $H(X|X^{n-1})$ для стационарных источников.

Кодовый алфавит. Кодовые слова. Равномерный код. Мощность кода. Скорость равномерного кода. Множество однозначно декодируемых последовательностей. Ошибка кодирования. Вероятность ошибки кодирования. Прямая теорема кодирования для дискретного постоянного источника. Обратная теорема кодирования для дискретного постоянного источника.

2 Неравномерное кодирование дискретных источников.

Постановка задачи неравномерного побуквенного кодирования. Свойство однозначной декодируемости. Неравномерный побуквенный код. Однозначно декодируемый код. Префиксный код. Кодовое дерево. Древовидный код. Средняя длина кодовых слов. Неравенство Крафта. Доказательство необходимости и достаточности. Прямая теорема побуквенного неравномерного кодирования. Обратная теорема побуквенного неравномерного кодирования.

3 Побуквенное кодирование.

Оптимальный побуквенный код – код Хаффмана. Свойства кодов. Алгоритм построения кодового дерева кода Хаффмана. Пример построения кода Хаффмана. Избыточность кода Хаффмана. Код Шеннона. Алгоритм построения кода Шеннона. Кодовое слово кода Шеннона. Кодовое дерево кода Шеннона. Графическая интерпретация кода Шеннона. Код Гилберта-Мура. Алгоритм построения кода Гилберта-Мура. Кодовое слово кода Гилберта-Мура. Графическая интерпретация кода Гилберта-Мура.

4 Неравномерное кодирование для стационарного источника.

Постановка задачи Неравномерное кодирование для стационарного источника. Средняя скорость кодирования для блоков длиной n. Обратная теорема неравномерного кодирования для стационарного источника. Прямая теорема неравномерного кодирования для стационарного источника. Арифметическое кодирование. Понятие лексикографического порядка. Вычисление кумулятивной вероятности. Рекуррентные формулы. Алгоритм арифметического кодирования. Графическая интерпретация арифметического кодирования. Алгоритм декодирования арифметического кода и некоторые аспекты практической реализации арифметического кодирования.

5 Алгоритмы кодирования источников, применяемые в архиваторах.

Монотонные коды. Унарный код. Код Голомба. Код Галлагера-Ван Вухриса. Код Левенштейна. Упрощенный код Левенштейна (код Элайеса). Теорема о роли монотонных кодов в универсальном кодировании. Интервальное кодирование и метод «стопка книг». Метод скользящего словаря (LZ-77). Формальное описание алгоритма скользящего словаря (LZ-77). Окно наблюдения (Объем скользящего словаря). Алгоритм работы кодера. Пример алгоритма LZ-77. Модификация LZ-77, предложенная Фиала и Гриине (LZFG). Алгоритм LZFG. Алгоритм LZW. Практические аспекты применения алгоритма скользящего словаря. Метод кодирования PPM. Схема алгоритма PPM. Варианты алгоритма PPM. Идея алгоритма PPM. Практическая реализация алгоритма PPM. Прямое преобразование Барроуза-Уилера. Пример использования алгоритма PPMD. Результаты преобразования. Обратное преобразование Барроуза-Уилера.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	3	Реализация алгоритма построения кодового дерева – кода Хаффмена.	2
2	3	Реализация алгоритма построения кода Шеннона.	2
3	3	Реализация алгоритма построения кода Гилберта-Мура.	2
4	3	Реализация алгоритма Арифметического кодирования.	2
5	3	Реализация алгоритма декодирования Арифметического кода.	2
6	4	Реализация регулярного неравномерного кода. Регулярный код Хафмена.	2
7	4	Сравнение алгоритмов монотонного кодирования	4
8	5	Реализация метода скользящего словаря LZ-77(модификации метода - алгоритма LZFG).	4
9	5	Реализация алгоритма PPM	4
10	5	Прямое преобразование Барроуза-Уилера.	4
11	5	Обратное преобразование Барроуза-Уилера.	4
12	5	Сравнение способов кодирования.	2
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1 Балюкевич Э. Л. Основы теории информации. Учебно-практическое пособие/ Балюкевич Э. Л. - Евразийский открытый институт, 2008. Университетская библиотека. Режим доступа - https://biblioclub.ru/index.php?page=book_red&id=90955.

2 Гультяева Т. А. Основы теории информации и криптографии. Конспект лекций / Новосибирск: НГТУ, 2010. Режим доступа – http://biblioclub.ru/index.php?page=book&id=228963.

5.2 Дополнительная литература

1 Игнатов, В. А. Теория информации и передачи сигналов: учеб. для вузов / В. А. Игнатов.- 2-е изд., перераб. и доп. - М. : Радио и связь, 1991. - 280 с.

2 Заельская, Н. А. Теория информации [Электронный ресурс] : электронный курс лекций / Н. А. Заельская; М-во науки и высш. образования Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбург. гос. ун-т". - Оренбург : ОГУ. - 2019. Режим доступа: https://ufer.osu.ru/index.php?option=com_uferdbsearch&view=uferdbsearch&action=details&ufer_id=2032

5.3 Периодические издания

1 Вестник компьютерных и информационных технологий: журнал. - М.: Агентство "Роспечать".

2 Информационные технологии: журнал. - М.: Агентство "Роспечать".

5.4 Интернет-ресурсы

www.citforum.ru/ - портал аналитических и научных статей в области информационных технологий;

www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»;

https://www.lektorium.tv/course/26243 - «Лекториум», МООК: «Введение в теорию информации».

Заельская, Н. А. Теория информации [Электронный ресурс] : электронный курс в системе Moodle / Н. А. Заельская; М-во науки и высш. образования Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбург. гос. ун-т". - Оренбург : ОГУ. - 2019. Режим доступа: https://moodle.osu.ru/course/view.php?id=935

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1 Операционная система Astra Linux. «Astra Linux Special Edition» РУСБ.10015-01, лицензионный договор №А-2021-1374-ВУЗ от 28.05.2021;

2 LibreOffice – свободно распространяемый офисный пакет, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.

3 Базы данных, информационно-справочные и поисковые системы:

- Консультант Плюс, Режим доступа: https://www.consultant.ru/cons/cgi/online.cgi
- Открытые поисковые системы: Yandex, Mail и др.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется компьютерный класс, оснащенный комплектами ученической мебели, доской и компьютерами с обеспечением доступа в электронную информационно-образовательную среду ОГУ.

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой, с обеспечением доступа в электронную информационно-образовательную среду ОГУ.

Каждый вид помещения может быть дополнен средствами обучения, реально используемыми при проведении учебных занятий соответствующего типа (например, - лабораторные стенды, макеты, имитационные модели, компьютерные тренажеры, симуляторы, муляжи, учебно-наглядные пособия, плакаты и т.п.)